The Commonwealth of Massachusetts
Motor Vehicle Insurance - Merit Rating Board
P.O. Box 55889, Boston, Massachusetts 02205-5889
(617) 267-3636 Fax (617) 351-9660

MARY ANN MULHALL
DIRECTOR

TO: Massachusetts Merit Rating Liaisons

FROM: Mary Ann Mulhall, Director

DATE: June 17, 2009

RE: More Secure Data Transfer Service

NOTICE NO: 0031

The MRB has created a more secure data transfer service to meet the requirements of Massachusetts security legislation (see MGL Chapter 93H and 201 CMR 17.00) and federal regulations for protecting personal information. This new data transfer service uses PGP encryption to protect personal information while data files are in transit and at rest on the MRB FTP site.

I'm enclosing "*Chapter 5: DATA TRANSFER WITH THE MRB"* of *Administrative Procedures for Safe Driver Insurance Plan* updated for the new service. Our conversion schedule and a summary of the changes are included below.

1. Schedule. Insurers may start converting to the new service immediately. Insurers should start their conversion by submitting test files using our testing procedures (see Chapter 5 Section 5.7) before submitting production files. The existing (old) server will remain in operation until September 30, 2009. Insurers must convert to the new service by this date.

2. Address of New Server. The IP address of this new server is: 208.218.131.232.

3. User Name, Password, and Folder Configuration. An insurer's username, password, and folder configuration on this (new) server are the same as the current (old) server.

4. File Encryption with PGP. Files transferred with the MRB must be encrypted using PGP encryption. The MRB will send the MRB PGP public key to the insurer. The insurer will need to create a PGP public/private key pair and send the public key to the MRB. The insurer will use the MRB's public key to encrypt a source file before it is uploaded to the insurer's Outbox folder on the MRB FTP site. The MRB will use the insurer's public key to encrypt a response file before it is uploaded to the insurer's Inbox folder on the MRB FTP site.

5. File Transfer Protocols. The PGP encrypted files may be transferred using FTP or SFTP (SSH). (Future: MRB will allow transfers using FTP over SSL if there is enough demand from insurers.)

-FTP. The FTP control port is 21, the active data port is 20, and the passive ports are 50000-50010.

-SFTP (SSH). SSH uses port 22 for both the control port and the data port. SSH data transfers use username and password authentication.

-(Future): FTP over SSL Using Implicit Mode. The control port for Implicit Mode FTP over SSL is 990. The passive ports are 50000-50010. Passive mode transfers are required.

6. File Naming Conventions. The names of PGP encrypted files transferred with the MRB must contain the PGP extension (.PGP). For example, the Policy Inquiry Source File SI090601.TXT should be encrypted to file SI090601.TXT.PGP. MRB will create the corresponding encrypted response to file RI090601.TXT.PGP.

Enclosures:
Chapter 5: DATA TRANSFER WITH THE MRB

Chapter 5
DATA TRANSFER WITH THE MRB

This chapter provides procedures for insurers to transfer files with the MRB.

Section 5.1 explains the use of the MRB FTP site, file encryption, file transfer protocols, and logging of insurer accesses.

Section 5.2 describes the file format requirements.

Section 5.3 describes user folders (directories) and the purpose of each folder.

Section 5.4 defines the naming convention for source files submitted by insurer users.

Section 5.5 defines the naming convention for response files created by the MRB.

Section 5.6 contains a file transfer example.

Section 5.7 explains testing procedures.

Section 5.1
General Information

5.1.1 Use of the MRB FTP Site. The MRB FTP site must be used for file transfer between the MRB and an insurer. Each insurer has a unique home folder (directory) on this MRB FTP site for file transfer with the MRB. A user's home folder may not be accessed or viewed by another user.

5.1.2 File Encryption with PGP. Files transferred with the MRB must be encrypted using PGP encryption. The MRB will send the MRB PGP public key to the insurer. The insurer will need to create a PGP public/private key pair and send the public key to the MRB. The insurer will use the MRB's public key to encrypt a source file before it is uploaded to the insurer's Outbox folder on the MRB FTP site. The MRB will use the insurer's public key to encrypt a response file before it is uploaded to the insurer's Inbox folder on the MRB FTP site.

5.1.3 File Transfer Protocols. The PGP encrypted files may be transferred using FTP or SFTP (SSH). (Future: MRB will allow transfers using FTP over SSL if there is enough demand from insurers.)

-FTP. The FTP control port is 21, the active data port is 20, and the passive ports are 50000-50010.

-SFTP (SSH). SSH uses port 22 for both the control port and the data port. SSH data transfers use username and password authentication.

-(Future): FTP over SSL Using Implicit Mode. The control port for Implicit Mode FTP over SSL is 990. The passive ports are 50000-50010. Passive mode transfers are required.

5.1.4 Logging.

Each user access to the MRB FTP site will be logged. The log will contain the username, the user IP Address, the date, the time of day, the number of bytes received, the number of bytes sent, the action (upload, download...), and the filename uploaded or downloaded.

Section 5.2
File Format Requirements

A source file from a user must be a fixed-width ASCII text file. Each record must be terminated by a carriage return (CHR$(13)) and a line feed (CHR$(10)). The ASCII text file must be encrypted using PGP encryption before the file is transferred to the insurer's Outbox folder on the MRB FTP site.

The response file created by the MRB will be a fixed-width ASCII text file. Each record will be terminated by a carriage return (CHR$(13)) and a line feed (CHR$(10)). MRB will encrypt the response file using PGP encryption before MRB uploads the file to the insurer's Inbox folder on the MRB FTP site.

The record format for each file transferred with the MRB is found in the Appendix listed below.

Appendix

Section 5.3
User Folders (Directories)

Each user has a home folder (directory) on the MRB FTP site with the same name as the user's username. The user's home folder contains an Inbox folder with subfolders and an Outbox folder with subfolders. A user uploads a source file to one of the Outbox subfolders and downloads an MRB response file from one of the Inbox subfolders. When a user logs on to the MRB FTP site, the user's current folder (directory) is the user's home folder (directory).

An outline of the user folders and a description of each folder follow. For any given user, the term, <username>, should be replaced by the user's username.

<username>
- Inbox
  - Badfile
  - CLM
  - CLMTest
  - INQ
  - INQTest
  - NTR
  - OOS
  - OOSTest
- Outbox
  - CLM
  - CLMTest
  - INQ
  - INQTest
  - OOS
  - OOSTest

/<username>/Inbox/Badfile folder. The MRB will put any source file that could not be processed by the MRB in this folder. The filename in this folder will be the same as the source filename submitted by the user.

/<username>/Inbox/CLM folder. This folder is for SDIP Claim Response files from the MRB. The MRB will put the SDIP Claim Response File in this folder. The user must download the file from this folder. After the file is downloaded, the user may delete the file or leave it for a few days as backup. Periodically, the MRB will purge any files in the user's Inbox/CLM folder that are over 15 days old.

/<username>/Inbox/CLMTest folder. This folder is for testing SDIP Claims. The MRB will put the test SDIP Claim Response File in this folder. The user must download the file from this folder. After the file is downloaded, the user may delete the file or leave it for a few days as backup. Periodically, the MRB will purge any files remaining in this folder.

/<username>/Inbox/INQ folder. This folder is for Policy Inquiry Response files from the MRB. The MRB will put the Policy Inquiry Response File in this folder. The user must download the file from this folder. After the file is downloaded, the user may delete the file or leave it for a few days as backup. Periodically, the MRB will purge any files in the user's Inbox/INQ folder that are over 15 days old.

/<username>/Inbox/INQTest folder. This folder is for testing Policy Inquiries. The MRB will put the test Inquiry Response File in this folder. The user must download the file from this folder. After the file is downloaded, the user may delete the file or leave it for a few days as backup. Periodically, the MRB will purge any files remaining in this folder.

/<username>/Inbox/NTR folder. This folder is for Notices to Reinquire from the MRB. The MRB will put the Notice to Reinquire File in this folder. The user must download the file from this folder. After the file is downloaded, the user may delete the file or leave it for a few days as backup. Periodically, the MRB will purge any files in the user's Inbox/NTR folder that are over 15 days old.

/<username>/Inbox/OOS folder. This folder is for Out-of-State Driving Record Response files from the MRB. The MRB will put the Out-of-State Driving Record Response File in this folder. The user must download the file from this folder. After the file is downloaded, the user may delete the file or leave it for a few days as backup. Periodically, the MRB will purge any files in the user's Inbox/OOS folder that are over 15 days old.

/<username>/Inbox/OOSTest folder. This folder is for testing Out-of-State Driving Records. The MRB will put the test Out-of-State Driving Record Response File in this folder. The user must download the file from this folder. After the file is downloaded, the user may delete the file or leave it for a few days as backup. Periodically, the MRB will purge any files remaining in this folder.

/<username>/Outbox/CLM folder. This folder is for SDIP Claim source files submitted by the user. The user must put an SDIP Claim Source File in this folder. The MRB will rename the file to a unique MRB internal name and then download the file for the MRB application. Periodically, the MRB will delete these renamed files.

/<username>/Outbox/CLMTest folder. This folder is for testing SDIP Claims. This folder is for test SDIP Claim Source Files submitted by the user. The user must put a test SDIP Claim Source File in this folder. The MRB will rename the file to a unique MRB internal name and then download the file for the MRB application. Periodically, the MRB will delete these renamed files.

/<username>/Outbox/INQ folder. This folder is for Policy Inquiry source files submitted by the user. The user must put a Policy Inquiry Source File in this folder. The MRB will rename the file to a unique MRB internal name and then download the file for the MRB application. Periodically, the MRB will delete these renamed files.

/<username>/Outbox/INQTest folder. This folder is for testing Policy Inquiries. This folder is for test Policy Inquiry source files submitted by the user. The user must put a test Policy Inquiry Source File in this folder. The MRB will rename the file to a unique MRB internal name and then download the file for the MRB application. Periodically, the MRB will delete these renamed files.

/<username>/Outbox/OOS folder. This folder is for Out-of-State Driving Record source files submitted by the user. The user must put an Out-of-State Driving Record Source File in this folder. The MRB will rename the file to a unique MRB internal name and then download the file for the MRB application. Periodically, the MRB will delete these renamed files.

/<username>/Outbox/OOSTest folder. This folder is for testing Out-of-State Driving Records. This folder is for test Out-of-State Driving Record Source Files submitted by the user. The user must put a test Out-of-State Driving Record Source File in this folder. The MRB will rename the file to a unique MRB internal name and then download the file for the MRB application. Periodically, the MRB will delete these renamed files.

Section 5.4
Naming Convention for Source Files Submitted by Insurer Users

A source file submitted by an insurer user must conform to the following naming convention.

(a) The filename must be eight (8) characters long followed by an extension of .TXT.PGP.

(b) The leftmost character must be "S". The character S identifies the file as a source file from a user.

(c) The second character from the left identifies the application:

C	SDIP Claim
I	Policy Inquiry
D	Out-of-State Driving Record

(d) The remaining six (6) characters are assigned by the user and may be any valid filename characters. An example for each application is included below.

(unencrypted)	(encrypted)	(application)
SCABC002.TXT	SCABC002.TXT.PGP	C
SIABC002.TXT	SIABC002.TXT.PGP	I
SDABC002.TXT	SDABC002.TXT.PGP	D

(e) An insurer should use a unique filename for each file submitted to the MRB. An insurer should not reuse the same filename.

Section 5.5
Naming Convention for Response Files Created by the MRB

For each application, the filename used by the MRB for a response file will be the same as the source filename submitted by the user with the leftmost character changed from an "S" to "R". The "R" indicates a response file created by the MRB. For example, if the user submits a Policy Inquiry Source File with the filename of SIXYZ005.TXT.PGP, then the MRB will create a Policy Inquiry Response File with the filename of RIXYZ005.TXT.PGP.

The Notice to Reinquire files created by the MRB will be named using the format **RNuuuuss.TXT.PGP** where uuuu is the user's username and ss is the MRB's Notice to Reinquire run sequence number for the year. For example, the Notice to Reinquire response file for user U444 created for the MRB's first Notice to Reinquire run of the year 2009 would be **RNU44401.TXT.PGP**.

Section 5.6
File Transfer Example

This example is a summary of the steps to upload a user source file and then download an MRB response file. This example for the Policy Inquiry application assumes a username of U444 and a source filename before encryption of SIABC002.TXT.

Step 1. User encrypts the source file, SIABC002.TXT, to SIABC002.TXT.PGP.

Step 2. User logs on to the MRB FTP site with the username assigned, in this example, U444, and the password assigned.

Step 3. User transfers the source file, SIABC002.TXT.PGP, to the /U444/Outbox/INQ folder.

Step 4. The MRB renames the file to a unique MRB internal name, and then downloads the file for the MRB Policy Inquiry application. The MRB downloads user source files periodically throughout the day.

Step 5. The MRB decrypts the source file, SIABC002.TXT.PGP, to SIABC002.TXT.

Step 6. The MRB checks the format of the source file, SIABC002.TXT. If the file format is valid, then processing continues with ***Step 7***. If the file format is bad, then MRB moves the encrypted source file, SIABC002.TXT.PGP, to the /U444/Inbox/Badfile folder.

(overnight)

Step 7. The MRB runs the Policy Inquiry Application that retrieves the operator's SDIP information, updates the driving records, and creates a Policy Inquiry Response File for each Policy Inquiry Source File processed.

Step 8. The MRB encrypts the response file, RIABC002.TXT, to RIABC002.TXT.PGP.

Step 9. The MRB moves the encrypted file to the /U444/Inbox/INQ folder.

(next business day)

Step 10. User logs on as described in ***Step 2*** above.

Step 11. User downloads the encrypted response file, RIABC002.TXT.PGP, from the /U444/Inbox/INQ folder.

Step 12. User decrypts the response file, RIABC002.TXT.PGP, to RIABC002.TXT.

Step 13. User may delete the response file, RIABC002.TXT.PGP, from the /U444/Inbox/INQ folder or leave it there for a few days as backup.

Section 5.7
Testing

A special test folder is created for system testing of each application. The MRB normally runs tests on each Tuesday and each Thursday. Insurers who upload a test file before noon on one of the two test days will receive a response the next morning.

During the test period, a user may upload a source file to the Outbox test folder for the appropriate application. For example, to test the Policy Inquiry Application, a user would upload a Policy Inquiry Source File to the **/<username>/Outbox/INQTest** folder. If the file format is bad, the MRB will place the source file in the **/<username>/Inbox/Badfile** folder. If the file format is valid, the MRB will process the source file using a test database and then place the Policy Inquiry Response File in the **/<username>/Inbox/INQTest** folder. The test database does not contain valid driving records and should not be used for an operator's SDIP information.

A test Policy Inquiry Source File should contain no more than 5,000 records. A test SDIP Claim Source File should contain no more than 500 records.